대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0083113
Application Number

출 원 년 월 일 : 2002년 12월 24일
Date of Application DEC 24, 2002

출 원 인 : 학교법인 한국정보통신학원
Applicant(s) INFORMATION AND COMMUNICATIONS UNIVERSITY EDUCATION/

2003 년 02 월 26 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0002
【제출일자】	2002.12.24
【발명의 명칭】	겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법
【발명의 영문명칭】	METHOD OF ID-BASED RING SIGNATURE BY USING BILINEAR PARINGS
【출원인】	
【명칭】	학교법인 한국정보통신학원
【출원인코드】	2-1999-038195-0
【대리인】	
【성명】	장성구
【대리인코드】	9-1998-000514-8
【포괄위임등록번호】	2000-005740-6
【대리인】	
【성명】	김원준
【대리인코드】	9-1998-000104-8
【포괄위임등록번호】	2000-005743-8
【발명자】	
【성명의 국문표기】	장 팡구오
【성명의 영문표기】	ZHANG,Fangguo
【주소】	대전광역시 유성구 화암동 58-4
【국적】	CN
【발명자】	
【성명의 국문표기】	김광조
【성명의 영문표기】	KIM,Kwang Jo
【주민등록번호】	560410-1347622
【우편번호】	302-773
【주소】	대전광역시 서구 둔산동 삼성한마루아파트 7-1406
【국적】	KR
【심사청구】	청구
【조기공개】	신청

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구 , 특허법 제64조의 규정에 의한 출원공개를 신청합니다. 대리인
장성구 (인) 대리인
김원준 (인)

【수수료】

【기본출원료】	19 면	29,000 원
【가산출원료】	0 면	0 원
【우선권주장료】	0 건	0 원
【심사청구료】	8 항	365,000 원
【합계】	394,000 원	
【감면사유】	학교	
【감면후 수수료】	197,000 원	

【첨부서류】 1. 요약서·명세서(도면)_1통 2.고등교육법 제2조에의한 학교임을 증명하는 서류[설립인가서]_1통

【요약서】

【요약】

본 발명은 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법에 관한 것으로, 원형 서명을 위해 시스템 매개변수를 생성하는 단계; 서명자가 요청한 ID_i 를 갖는 서명자의 공개키와 비밀키를 계산하는 단계; 서명자가 G 에 속하는 임의의 값 A 를 생성하여 원형서명의 초기값 c_{k+1} 을 계산하는 단계; 원형서명의 초기값에 대하여 난수 G 에 속하는 임의의 T_i를 선택하고, 연속된 추가 원형 서명 값 c_{i+1}을 계산하는 단계; 추가 원형 서명 값 c_{i+1}에 대하여 서명자 자신의 비밀키를 이용하여 원형 서명값 T_k를 계산하는 단계; 서명자가 n+1 개의 원형 서명값을 정의하여 검증자에게 전송하는 단계; 서명자로부터 제공받은 원형 서명에서 은닉 정보를 제거하여 원형 서명을 복구하는 단계; 원형 서명의 정당성을 검증하는 단계를 포함한다. 따라서, 기존의 방법과 달리 공개적으로 용이하게 취득할 수 있는 사용자의 개인식별정보를 이용하므로 인증기관에 대한 절대적 의존성을 탈피할 수 있는 효과가 있다.

【대표도】

도 2

【명세서】

【발명의 명칭】

겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법{METHOD OF ID-BASED RING SIGNATURE BY USING BILINEAR PARINGS}

【도면의 간단한 설명】

도 1은 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법을 수행하기 위한 블록 구성도이고,

도 2는 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법에 대한 상세 흐름도이다.

<도면의 주요부분에 대한 부호의 설명>

100 : 서명자 200 : 검증자

300 : 신뢰기관(또는, 키생성 센터)

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법에 관한 것으로, 특히 그룹 전자 서명 기법을 단순화시켜 그룹 관리자 없이도 복수의 사용자로만 구성되는 원형서명에 있어서, 타원곡선 군에서 성립되는 겹선형 쌍(Bilinear Pairings)을 이용하여 사용의 개인식별정보에 기반하고 있는 암호학적으로 안전하게 하는 원형서명 방법에 관한 것이다.

<7> 통상적으로, 정보통신망의 발전과 더불어 다양한 정보가 사이버 공간을 통하여 전달되고 있다. 송신자가 전자 우편이나 전자 문서 전달 시스템 등을 통하여 귀중한 메시지를 전달하고자 할 때, 메시지 송신자의 입장에서는 정당한 수신자가 정보를 제대로 받았는지, 그리고 수신자의 입장에서는 메시지의 생성자가 정당한 송신자가 맞는지 등을 확인할 메커니즘이 필요하다.

<8> 이러한 기능을 효과적으로 제공하기 위한 방법 중의 하나로 각 사용자가 2개의 키 정보로서 비밀키와 공개키를 가지고 있는 공개키 암호 시스템을 이용한 전자 서명 방식이 이용되고 있다.

<9> 즉, 공개키 암호 시스템의 가장 중요한 응용의 하나인 전자서명은 문서의 서명자 또는 메시지의 생성자의 신분을 확인하거나 메시지나 문서의 원본이 변경되지 않았다는 것을 보증하기 위해서 사용된다. 전자서명은 인터넷 기반의 거래나 전자상거래에 있어서 핵심 요소로서 부수적인 특수 목적을 위해서 특정 요구사항이 서명기법에 추가 될 수 있다.

<10> 일반적으로, 서명자의 익명성은 원형전자서명(Ring Digital Signature) 또는 그룹 전자서명(Group Digital Signature)에 의해서 제공되며 원형전자서명 또는 간단히 원형 서명은 부가기능을 갖는 매우 중요한 전자서명기법이다.

<11> 원형 서명의 개념은 아시아크립토 2001 학회에서 리베스트(R. Rivest), 샤미르(A. Shamir), 및 타우만(Y. Tauman)에 의해서 제안되었다. 그들이 제안한 원형서명 기법은 그룹 관리자가 없이 사용자만으로 구성된 단순화된 그룹서명으로 간주할 수 있다. 원형 서명 기법에서 검증자는 원형의 구성원에 의해서 서명되었다는 것을 검증할 수는 있으나 서명자를 알 수는 없으므로 서명자의 익명성을 보장할 수 있다.

<12> 그룹 서명과 달리, 원형서명은 그룹 관리자, 초기화 절차, 철회 절차 및 구성원 조정이 요구되지 않는다. 사용자는 누구나 자신을 포함하여 가능한 서명자의 그룹을 선택할 수 있다. 사용자는 자신의 비밀키와 다른 구성원의 공개키를 사용하여 메시지에 서명하며, 이 서명과정에서 다른 사용자의 승인이나 검증 절차가 필요 없다.

<13> 원형서명 기법은 익명성의 보장의 한 방법으로 신뢰할 수 있는 정보를 제시하거나 지정된 수신자만 볼 수 있는 전자 메일을 서명하는 등의 다자간 연산과 관련된 문제를 해결할 수 있는 기법이다. 또한 서명자의 익명성을 철회시킬 수 있는 방법이 존재하지 않는다. 원형서명은 그룹을 가변적으로 형성할 수 있게 하며 통상 특수한 초기화 절차를 요구하지 않으며 리베스트-샤미르-타우만에 의해서 제안된 원형서명 방식은 일반적인 공개키 기반구조 하에서 동작한다.

<14> 공개키 시스템에서는 각 사용자는 공개키와 비밀키 쌍을 갖는다. 사용자의 공개키와 소유자 정보는 전자 인증서에 의해서 연결된다. 그래서 현재의 공개키 기반구조는 복잡한 인증기관, 막대한 통신비용 및 인증서 확인을 위해 요구되는 계산비용 등에 대해서는 이미 잘 알려진 사실이다. 그러나 중요한 문제는 모든 인증서는 공개이고 모든 사용자가 접근할 수 있다는 기본가정이다. 이 가정이 언제나 실현 가능한 것은 아니라는 사실이다.

<15> 특히 무선 네트워크에서 네트워크 연결은 대단히 비쌀 수가 있다. 인증서 기반 시스템에서 사용자의 공개키를 사용하기 전에 프로토콜 참여자는 먼저 그 사용자의 인증서를 확인해야 한다. 결국, 이 시스템은 많은 계산시간과 사용자 증가에 따라 방대한 양의 저장 공간을 요구한다.

<16> 1984년 샤미르(Shamir)는 개인식별정보 기반의 공개키 암호라는 새로운 개념을 제안했다. 즉, 개인식별정보 기반의 공개키 암호는 개인식별정보와 공개키 간의 일대일 사상이 구축되게 함으로써 기존 공개키 관리 방식이 대단히 경제적으로 구축이 가능하다. 그래서 개인식별정보 기반 암호는 공개키 인증서와 인증기관에 대한 필요성뿐 만 아니라 의존성도 줄일 수 가 있다. 개인식별정보·기반 공개키 암호는 사용자를 특정화할 수 있는 개인의 전자 우편 주소나 전화번호 같은 임의의 식별 값으로부터 공개키를 유도할 수 있기 때문에 공개키 암호 시스템을 구축하거나 전자 서명을 생성하는 데 대단히 유용한 암호학적 도구이다. 동시에 개인식별정보 기반 방법은 공개키 인증서의 필요성과 수를 줄일 수 있도록 하기 때문에 키 관리 시스템이 대단히 용이하게 구축된다.

<17> 겹선형 쌍들, 즉, 대수 곡선 상의 베일(Weil) 쌍과 테이트(Tate) 쌍은 대수기하학 연구에서 매우 중요한 도구들이다. 암호에서 겹선형 쌍의 초기 응용은 이산대수문제(Discrete Logarithm Problem)의 평가를 위한 것이었다. 예를 들면, 베일 쌍을 사용한 엠오브이(MOV) 공격이나 테이트 쌍을 이용한 에프아르(FR) 공격은 특정 타원곡선이나 초타원곡선에서의 이산대수문제를 유한체에서의 이산대수문제로 간단히 축약이 가능하게 한다. 그러나 최근에 겹선형 쌍들이 암호에서 다양한 응용분야가 있다는 것이 밝혀졌다. 예들 들면, 보네-프랭크린(Boneh-Franklin)의 개인식별정보 기반 암호 시스템, 스마트 카드의 개인식별정보 기반 인증 키관리 관리와 몇 가지 개인식별정보 기반 전자서명 기법을 들 수 있다.

<18> 개인식별정보 기반의 원형서명은 일반 원형서명과 개인식별 기반 기법을 결합한 형태로 검증을 하기 위한 공개키가 서명자의 개인식별정보가 되는 것이다. 즉, 개인식별

정보 기반의 원형서명은 서명자의 공개키가 단순히 그의 개인식별정보이기 때문에 서명 과정이 대단히 효율적이다.

<19> 크립토 2001 학회에서 최초로 보네와 프랭크린에 의해서 겹선성 사상을 갖는 군(Group)의 특성을 사용한 암호 시스템이 제안된 후 암호 및 복호화 기법, 키합의 및 키 동의 기법, 서명기법 등이 제안되었으나 개인식별정보 기반의 공개키 구조에서 필수적인 개인식별정보 기반의 원형서명 기법이 제안되어 있지 아니하다는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<20> 따라서, 본 발명은 상술한 문제점을 해결하기 위해 안출한 것으로서, 그 목적은 개인식별정보 기반 공개키 암호시스템의 필수 항목의 하나인 개인식별정보 기반 원형서명 기법을 베일 쌍이나 테이트 쌍과 같은 겹선형 쌍을 사용하여 안전성과 익명성을 제공하는 새로운 개인식별정보 기반 원형서명 기법을 제안할 수 있도록 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법을 제공함에 있다.

<21> 상술한 목적을 달성하기 위한 본 발명에서 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법은 원형 서명을 위해 시스템 매개변수를 생성하는 단계; 서명자가 요청한 ID_i 를 갖는 서명자의 공개키와 비밀키를 계산하는 단계; 서명자가 G 에 속하는 임의의 값 A 를 생성하여 원형서명의 초기값 c_{k+1} 을 계산하는 단계; 원형서명의 초기값에 대하여 난수 G 에 속하는 임의의 T_i를 선택하고, 연속된 추가 원형 서명 값 c_{i+1}을 계산하는 단계; 추가 원형 서명 값 c_{i+1}에 대하여 서명자 자신의 비밀키를 이용하여 원형 서명 값 T_k를 계산하는 단계; 서명자가 n+1 개의 원형 서명값을 정의하여 검증자에게 전송하는 단계; 서명자로부터 제공받은 원형 서명에서 은닉 정보를 제거하여 원형 서명을 복구하는 단계; 원형 서명의 정당성을 검증하는 단계를 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<22> 이하, 첨부된 도면을 참조하여 본 발명에 따른 일 실시 예를 상세하게 설명하기로 한다.

<23> 도 1은 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법을 수행하기 위한 블록 구성도로서, 도 1a는 원형서명 기법의 주 참여자인 서명자(100)와, 검증자(200) 및 신뢰기관(300)을 포함한다.

<24> 서명자(100)는 주어진 시스템 매개변수에 따라 신뢰기관(300)이 제공하는 공개키와 비밀키를 사용하여 검증자(200)가 요구하는 메시지에 대하여 메시지의 내용을 모른 체 원형서명을 계산하여 검증자(200)에게 전송하는 역할을 담당한다.

<25> 검증자(200)는 서명자(100)에게 제시할 메시지를 은닉하고 서명자(100)로부터 제공받은 원형서명에 대한 서명을 계산하는 역할을 담당한다. 검증자(200)의 메시지와, 서명자(100)가 제시한 원형서명에서 추출한 서명 값으로부터 정당성을 검증할 수 있다.

<26> 신뢰기관(300)은 각 참여자가 모두 사용할 수 있는 시스템 매개변수를 생성하여 공개하고 각 참여자의 개인식별정보를 바탕으로 각각의 공개키와 비밀키를 생성하여 안전한 채널로 제공하는 역할을 담당한다. 여기서, 신뢰기관(300)은 시스템 초기화 시에만 참여하고 서명에는 참여하지 않는다.

<27> 도 1a 내지 도 1c에 대하여 보다 상세하게 설명하면, 상술한 참여자(서명자(100), 검증자(200), 신뢰기관(300))로 구성된 본 발명의 원형서명 기법은 도 1a의 시스템 매개변수와 마스터 키 생성과정 및 서명자(100)의 공개키와 비밀키 생성과정과, 도 1b의 서명자(100)와 검증자(200)간에 서명 및 서명 검증 과정과, 도 1c의 검증자(200)가

서명자(100)의 서명의 유효성을 검증하는 과정을 통하여 동작하는 것으로, 본 발명은 검증자(200)가 서명자(100)의 서명을 최종적으로 확인하는 기법과 관련된다.

<28> 도 2의 흐름도를 참조하면서, 상술한 구성을 바탕으로 본 발명에 따른 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법에 대하여 보다 상세하게 설명한다.

<29> 먼저, 시스템 매개변수 생성과정으로서, 서명자(100) 및 검증자(200) 모두가 공유하는 시스템 매개변수들이 신뢰기관(300)에 의해서 생성되어 공개된다(단계 201).

<30> 이러한 과정에서 임의의 순환군 G 와 V 가 생성되며, G 와 V 의 위수는 모두 q 이다. 위수가 q 인 타원곡선상의 점들의 군 G 와 역시 위수가 q 인 유한체 또는 곱셈 순환군 V 를 생성한다. 일반적으로 VZ_q^*에 해당되며, 수학식 1과 같은 겹선형 사상 e 를 정의한다.

<31> 【수학식 1】 $e:G\times G\mapsto V$

<32> 여기서, G 는 타원 곡선군 또는 초타원 곡선 자코비언(Jacobian)이며, V 는 곱셈 순환군 Z_q^*을 사용한다.

<33> 다음으로, 신뢰기관(300)은 마스터키로 에 속하는 임의의 정수 s 을 선택하고 $P_{pub}=sP$ 을 계산한다. 추가로 수학식 2의 사상을 만족하는 암호학적 해시 함수 H,H_1 을 생성한다.

<34> 【수학식 2】 $H:\{0,1\}^*\mapsto Z_q^*,H_1:\{0,1\}^*\mapsto G$

<35> 그 다음 단계로서, 신뢰기관(300)은 시스템 매개변수로서

$<G,q,P,P_{pub},H,H_1>$ 을 공개하고 s 을 마스터키로 사용하며, 시스템 매개변수와 마스터키를 사용하여 서명자(100)의 개인식별정보 ID_i 를 사용하여 신뢰기관(300) 자신의 공개키 P_{pub} 를 수학식 3을 사용하여 계산한다(단계 202).

<36> 【수학식 3】 $P_{pub}=s \cdot P$

<37> 이후, 신뢰기관(300)은 개인식별정보로 ID_i 를 갖는 서명자(100)가 비밀키와 공개키 생성을 요청하면, 수학식 4를 사용하여 해당 서명자(100)의 공개키 를 생성하고, 수학식 5를 사용하여 비밀키 를 생성하여 안전한 채널로 전송한다(단계 203).

<38> 【수학식 4】

<39> 【수학식 5】

<40> 다음으로, 원형서명 과정으로, 원형서명을 얻고자 하는 메시지를 m 이라 한 다음에, 서명자(100)는 G 에 속하는 임의의 값 A 를 선택하고, 메시지 m 과 개인식별정보의 집합 L 을 이용하여 수학식 6을 통해 원형서명의 초기값 을 계산한다(단계 204).

<41> 【수학식 6】

<42> 그 다음으로, 서명자(100)는 에 대하여, G 에 속하는 임의의 를 선택하고 수학식 7을 사용하여 연속된 추가 원형 서명 값 c_{i+1} 을 계산한다(단계 205).

<43> 【수학식 7】 $c_{i+1}=H(Lme(T_i,P)e(c_iH_1(ID_i),P_{pub}))$

<44> 이후, 서명자(100)는 자신의 비밀키 쌍을 이용하여 원형 서명값 T_k 를 수학식 8을 사용하여 계산한다(단계 206).

<45> 【수학식 8】 $T_k=A-c_kS_{ID_k}$

<46> 다음 단계로서, 서명자(100)가 검증자(200)에게 수학식 9와 같은 n+1 개의 원형 서명값을 정의하여 전송한다(단계 207).

<47> 【수학식 9】 $(c_0,T_0,T_1,\cdots,T_{n-1})$

<48> 검증하는 단계로서, 검증자(200)가 서명의 정당성을 수학식 10 및 수학식 11을 사용하여 검증한다(단계 208).

<49> 상기 검증 단계(208)에서 $i=0,\ldots,n-1$ 이며 $c_n=c_0$ 이면 정당한 서명이며(단계 209), 상기 검증 단계(208)에서 $i=0,\ldots,n-1$ 이 아니며 $c_n=c_0$ 이 아니면 서명을 거부한다(단계 210).

<50> 【수학식 10】 $c_{i+1}=H(Lme(T_i,P)e(c_iH_1(ID_i),P_{pub}))$

<51> 【수학식 11】 $H(m,e(S',P)\cdot e(Q_{ID},P_{pub})^{-c'})$

<52> $=H(m,e(S+aP_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$

<53> $=H(m,e(cS_{ID}+rP_{pub}+aP_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$

<54> $=H(m,e(cS_{ID},P)\cdot e(rP_{pub}+aP_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$

<55> $=H(m,e(S_{ID},P)^c\cdot e((r+a)P_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$

<56> $=H(m,e(Q_{ID},P_{pub})^c\cdot e((r+a)P,P_{pub})\cdot e(Q_{ID},P_{pub})^{-c'})$

<57> $=H(m,e(Q_{ID},P_{pub})^{c-c'} \cdot e(R+aP,P_{pub}))$

<58> $=H(m,e(Q_{ID},P_{pub})^{b} \cdot e(R+aP,P_{pub}))$

<59> $=H(m,e(bQ_{ID}+R+aP,P_{pub}))=c-b \pmod{q}=c'$

<60> 상술한 바와 같이, 본 발명에 따른 원형서명 기법을 이용하면 서명자(100)는 자신의 익명성뿐만 아니라 위조불가능성도 만족하는 효율적인 원형서명을 자신의 개인식별정보를 이용하는 시스템에서 수행할 수 있다.

【발명의 효과】

<61> 이상에서 설명한 바와 같이, 본 발명은 겹선형 쌍을 사용하여 개인식별정보 기반의 안전한 원형서명을 제공함으로써, 인증서 기반의 공개키 기반 구조가 내재하고 있는 단점을 극복하기 위해 개인식별정보 기반의 공개키 기반 구조가 활발하게 연구되고 있으며 공개키 기반 구조를 포함한 다양한 응용에서 개인식별정보 기반의 원형서명은 필수요소이다.

<62> 또한, 겹선형 사상을 이용한 본 원형서명은 기존의 방법과 달리 공개적으로 용이하게 취득할 수 있는 사용자의 개인식별정보를 이용하므로 인증기관에 대한 절대적 의존성을 탈피할 수 있다.

<63> 특히, 겹선형 사상은 테이트 쌍이나 베일 쌍을 타원곡선 상에서 구현하여 사용하였다. 이때 테이트 쌍이나 베일 쌍의 계산이 상대적으로 복잡하여 연산의 비효율성이 지적되었지만, 현재 암호학자들의 지속적인 연구로 인하여 연산 시간 개선이 꾸준히 이루어지고 있으며 최근에는 계산량을 줄이는 알고리즘의 연구에 힘입어 테이트 쌍이나 베일 쌍의 연산도 매우 효율적으로 계산되는 효과가 있다.

【특허청구범위】

【청구항 1】

서명자, 검증자 및 신뢰기관으로 구성된 시스템에서의 원형서명 방법에 있어서,

상기 원형 서명을 위해 시스템 매개변수를 생성하는 단계;

상기 서명자가 요청한 ID_i 를 갖는 서명자의 공개키와 비밀키를 계산하는 단계;

상기 서명자가 G 에 속하는 임의의 값 A 를 생성하여 원형서명의 초기값 을 계산하는 단계;

상기 원형서명의 초기값에 대하여 난수 G 에 속하는 임의의 T_i 를 선택하고, 연속된 추가 원형 서명 값 c_{i+1} 을 계산하는 단계;

상기 추가 원형 서명 값 c_{i+1} 에 대하여 상기 서명자 자신의 비밀키를 이용하여 원형 서명값 T_k 를 계산하는 단계;

상기 서명자가 n+1 개의 원형 서명값을 정의하여 검증자에게 전송하는 단계;

상기 서명자로부터 제공받은 원형 서명에서 은닉 정보를 제거하여 원형 서명을 복구하는 단계;

상기 원형 서명의 정당성을 검증하는 단계를 포함하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【청구항 2】

제 1 항에 있어서,

상기 신뢰기관에서 자신의 마스터키 s 을 선택하고 $P_{pub}=sP$ 을 계산하여 자신의 공개키로 사용하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【청구항 3】

제 1 항에 있어서,

상기 서명자가 요청한 ID_i 를 갖는 서명자가 키 생성을 요청할 경우, 상기 신뢰기관은 자신의 마스터키 s 을 사용하여 서명자의 공개키 $Q_{ID}=H_1(ID)$ 와, 비밀키 $S_{ID}=s \cdot Q_{ID}$ 을 계산하여 안전한 채널로 전송하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【청구항 4】

제 1 항에 있어서,

상기 원형서명의 초기값 c_{k+1} 은,

$c_{k+1}=H(Lme(A,P))$ 의 수학식에 의해 계산되는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【청구항 5】

제 1 항에 있어서,

상기 서명자가 $i=k+1,...,n-1,0,1,k-1$ 에 대하여, 연속된 추가 원형 서명 값 c_{i+1} 은,

$c_{i+1}=H(Lme(T_i,P)e(c_iH_1(ID_i),P_{pub}))$ 의 수학식에 의해 계산되는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【청구항 6】

제 1 항에 있어서,

상기 원형 서명값 T_k 는,

$T_k=A-c_kS_{ID_k}$ 의 수학식에 의해 계산되는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【청구항 7】

제 1 항에 있어서,

상기 n+1 개의 원형 서명값은,

$(c_0,T_0,T_1,\cdots,T_{n-1})$ 의 수학식에 의해 정의되는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【청구항 8】

제 1 항에 있어서,

상기 원형 서명의 정당성을 검증하는 단계는,

$c_{i+1}=H(Lme(T_i,P)e(c_iH_1(ID_i),P_{pub}))$ 의 수학식 및

$H(m,e(S',P)\cdot e(Q_{ID},P_{pub})^{-c'})$

$$=H(m,e(cS_{ID},P)\cdot e(rP_{pub}+aP_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(S_{ID},P)^{c}\cdot e((r+a)P_{pub},P)\cdot e(Q_{ID},P_{pub})^{-c'})$$

$$=H(m,e(Q_{ID},P_{pub})^{c}\cdot e((r+a)P,P_{pub})\cdot e(Q_{ID},P_{pub})^{-c'})$$

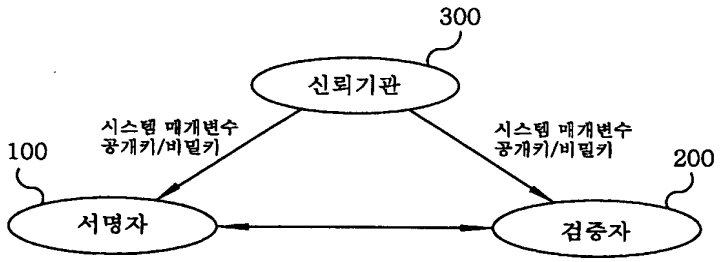
$$=H(m,e(Q_{ID},P_{pub})^{c-c'}\cdot e(R+aP,P_{pub}))$$

$$=H(m,e(Q_{ID},P_{pub})^{b}\cdot e(R+aP,P_{pub}))$$

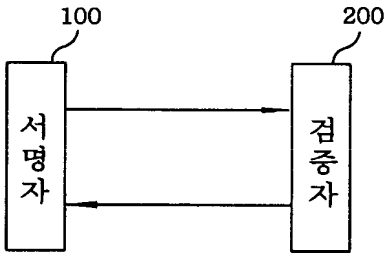
$=H(m,e(bQ_{ID}+R+aP,P_{pub}))=c-b\,(\mathrm{mod}\,q)=c'$ 의 수학식에 의해 이루어지며, 상기 검증 단계에서 $i=0,\ldots,n-1$ 이며 $c_n=c_0$ 이면 정당한 서명이며, 그렇지 않으면, 서명을 거부하는 것을 특징으로 하는 겹선형쌍을 이용한 개인식별정보 기반의 원형서명 방법.

【도면】

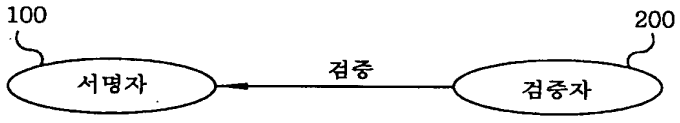
【도 1a】



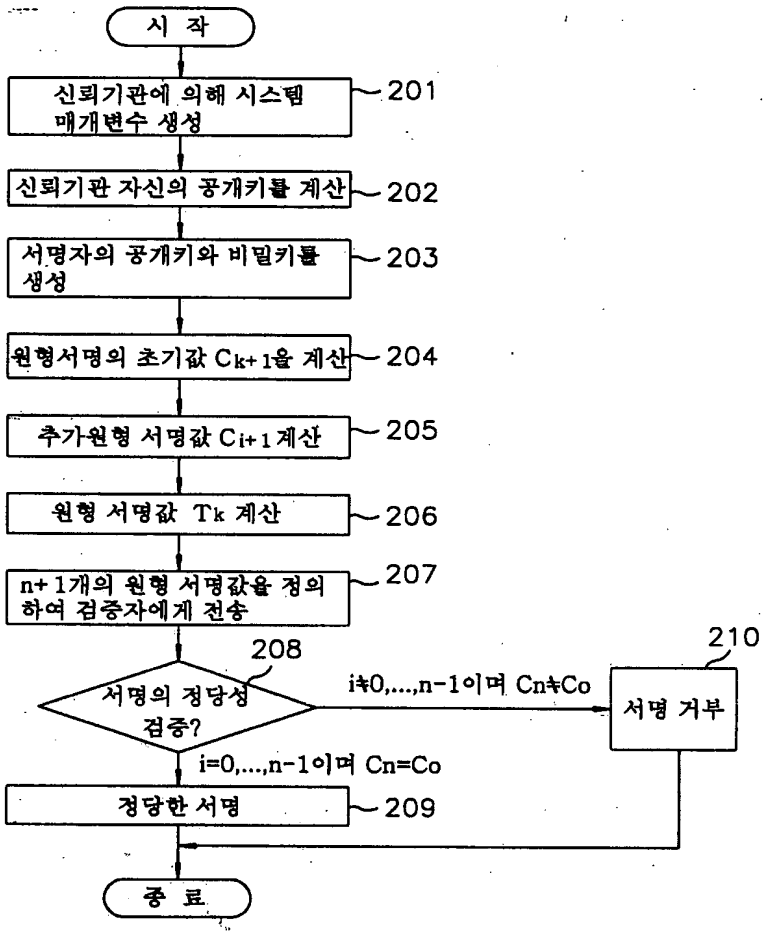
【도 1b】



【도 1c】



【도 2】


시 작
신뢰기관에 의해 시스템 매개변수 생성
201
신뢰기관 자신의 공개키를 계산
202
서명자의 공개키와 비밀키를 생성
203
원형서명의 초기값 Ck+1을 계산
204
추가원형 서명값 Ci+1 계산
205
원형 서명값 Tk 계산
206
n+1개의 원형 서명값을 정의하여 검증자에게 전송
207
208
서명의 정당성 검증?
i≠0,...,n-1이며 Cn≠Co
210
서명 거부
i=0,...,n-1이며 Cn=Co
정당한 서명
209
종 료